U.S. Department of Justice

Office of Legislative Affairs

Washington, D.C. 20530

February 13, 2004

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Enclosed please find responses to questions posed by the Committee to the Attorney General following the Committee's hearing of June 5, 2003, concerning oversight of the Department of Justice. Our responses are divided into two parts: those concerned with implementation of the USA PATRIOT Act and those concerning other matters.

We regret the delay in responding but hope that this information will prove helpful to you. If we may be of additional assistance in connection with this or any other matter, we trust that you will not hesitate to call upon us.

Sincerely,

William E. Moschella

William E. Moschella
Assistant Attorney General

Enclosures

cc: The Honorable John Conyers, Jr.
Ranking Minority Member

DEPARTMENT OF JUSTICE RESPONSES TO QUESTIONS FOR THE RECORD CONCERNING THE USA PATRIOT ACT (P.L. 107-56)

COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

JUNE 5, 2003

1. **The Department had previously advised this Committee that the FBI and the Department were taking additional steps to improve the efficiency of the Foreign Intelligence Surveillance Act (FISA) process. One of these steps was the creation of a FISA unit in November 2002, at FBI Headquarters that was charged with instituting an automated tracking system that would electronically connect the field divisions, FBI Headquarters, the FBI's National Security Law Unit, and the Office of Intelligence Policy Review (OIPR).**

   A. **What is the status of this automated tracking system?**

Answer: The FBI's automated tracking system, called the Foreign Intelligence Surveillance Act Management System (FISAMS), is being developed under a contract let in early 2003. Work began in February 2003 with a goal of having a pilot system available for testing in July 2003 and an Initial Operating Capability in October 2003.

The prototype system was fielded and tested by users in the field offices and at FBI Headquarters in July 2003 using test data sets. Feedback was used to modify the system and guide further development.

In October 2003, the contractor delivered Version 1.0 of the system for certification and accreditation testing by the Security Division. The FISAMS application was approved in November but the FBI's Information Resources Division (IRD) encountered a problem with portions of the operating system supporting the FISAMS, requiring testing of updated operating system software to correct this problem. IRD is working to provide to DOJ's Office of Intelligence Policy Review connectivity to the FBI production environment. Once these tasks are completed and the FISAMS is available on the production servers, the Security Division will issue approval to operate and the Foreign Intelligence Surveillance Act (FISA) Unit can begin to load the organizational structures and users into the system so actual operational use of the production system can begin.

During December 2003, the FISA Unit, Office of the General Counsel, FBI, conducted user training for FBI Headquarters and the Washington Field Office. Training for other field offices will take place starting in January 2004.

In addition, the contractor is developing Version 2.0 of the system, which will provide additional user features and an enhanced database. IRD is hiring two Information Technology Specialists

who will be dedicated to further development of the system in the coming years. In the future, the FBI plans to explore the use of electronic signatures for documents, electronic filing with the Foreign Intelligence Surveillance Court (FISC), and electronic distribution of court orders to common carriers and service providers.

B. What are the other duties of the FISA unit?

Answer: The FISA Unit performs the administrative support functions for the FISA process. In addition to FISA processing and tracking, which will be handled by the FISAMS, the FISA Unit is responsible for distribution of all FISC orders and warrants to the appropriate field divisions for their use and for service upon telecommunications carriers, Internet service providers, and other specified persons.

C. Has operational efficiency improved since the Unit was created?

Answer: Yes. The FISA Unit, the Office of Intelligence Policy and Review (OIPR), and the Foreign Intelligence Surveillance Court (FISC) have all taken steps to improve the distribution of orders and warrants after the court approves them.

At the direction of the Presiding Judge of the FISC, the Clerk of the Court changed the post-court processing of dockets. The Clerk of the Court now targets return of signed dockets to OIPR by close of business the next business day after approval. Previously, dockets could take up to a week or more to be returned to OIPR and the FBI.

OIPR has designated one employee as the Docket Clerk. The Docket Clerk is the only employee who is authorized to pick up signed dockets from the Clerk of the Court. This has given the Clerk of the Court a single point of contact for delivery of dockets and has helped ensure that all dockets are processed expeditiously upon receipt. Previously, dockets were returned to a number of attorneys and staff at OIPR and the FBI which led to inconsistent processing and distribution.

The FISA Unit has begun machine scanning primary and secondary orders and warrants upon receipt and e-mailing the resulting files to field office case agents for their use and to personnel in the various field offices for service of the secondary orders upon carriers, service providers, and other specified persons. We have found that most carriers and service providers will accept a printed copy of the signed, scanned document to renew coverage on an existing target. The conformed copies of the orders and warrants, with the raised seals, are subsequently sent for follow-up service and service to establish initial coverage on targets. Previously, machine copies of orders and warrants were made and communications prepared for distribution. This process often took up to two weeks.

These changes together have resulted in having a serviceable copy of a signed order in the hands of a carrier or service provider in a matter of two or three days rather than two or three weeks.

D. What other steps have been implemented to achieve optimum efficiency in the FISA application process?

Answer: Effective March 1, 2003, field offices began using a standard "FISA Request Form" to request initiation, renewal and modification of FISA coverage. This single, standard form replaced a variety of communications used in the past to request coverage. The form helps ensure that the drafters of the FISA packages receive all pertinent information required without additional, unnecessary administrative details, which facilitates quicker drafting.

Also effective March 1, 2003, field offices began sending requests to renew and amend existing FISAs directly to OIPR. Previously, all requests to renew or amend existing FISAs had to come through FBIHQ for approval prior to being sent to OIPR for drafting.

2. Section 326 of the USA PATRIOT ACT requires financial institutions to implement reasonable procedures to verify the identity of any person seeking to open a bank account. The Treasury Department has promulgated regulations that would permit these institutions to accept identification cards issued by embassies and consulates of foreign governments, which can be susceptible to fraud. What is the DOJ's position on the Treasury Department's implementation of section 326 of the USA PATRIOT Act?

Answer: On July 1, 2003, the Treasury Department issued a Notice of Inquiry regarding implementation of, and possible changes to, regulations promulgated pursuant to section 326 of the USA PATRIOT Act. On July 31, 2003, the Justice Department submitted comments to the Treasury Department regarding its Notice of Inquiry. Copies of those comments are enclosed. On September 25, 2003, the Treasury terminated its Notice of Inquiry and did not adopt the changes suggested by the Department of Justice.

3. Has the United States Department of Justice offered any classified evidence in immigration proceedings that have been instituted since September 11, 2001?

Answer: The Department of Justice has not offered classified evidence in any immigration proceeding initiated between September 11, 2001, and March 1, 2003, when responsibility to bring charges and present evidence in immigration proceedings transferred to the Department of Homeland Security.

4. In May 2003, the Justice Department published an interim regulation that provided a mechanism for the government to ask an immigration judge to place a "protective order" upon information that, while not classified, was sensitive and could damage

law enforcement or national security interests if released beyond parties to a specific immigration case.

a. What are the government's concerns that prompted it to authorize protective orders in immigration cases?

b. Is this "protective order" mechanism the Justice Department's alternative to closed hearings?

Answer: In promulgating the protective order rule, 28 CFR 1003.46, the Department of Justice was concerned that it would be necessary to present sensitive, non-classified law enforcement or intelligence documents to an immigration judge for consideration in removal proceedings. The rules of procedure before immigration judges at that time did not include any provision for protective orders, such as has long been the case with the Federal Rules of Civil Procedure. *See* F.R.Civ. P. Rule 26(c).

The protective order rule authorizes immigration judges to issue protective orders and accept documents under seal. This authority ensures that sensitive law enforcement or national security information can be protected from broad public dissemination, while still affording full use of the information by immigration judges, the Board of Immigration Appeals (BIA), respondents, the Department of Homeland Security (DHS), and reviewing courts. The rule sets out procedures for the DHS to seek protective orders and to appeal the denial of such requests. This rule also provides for sanctions for violations of protective orders. The rule applies in all immigration proceedings before the immigration judges and the BIA.

Protective orders are a complement to possible closed hearings. As a general proposition, the protective order under 8 CFR 1003.46 limits the dissemination of sensitive, unclassified law enforcement or intelligence documentary evidence or knowledged gained from that documentary evidence. Closure of a hearing – as is common in cases involving arriving aliens, abused spouses, and asylum seekers under 8 CFR 1003.27 and 1240.10 – is intended to protect the testimony of specific individuals. Of course, a protective order that will be discussed during a hearing necessitates that the hearing be closed.

c. In how many cases have protective orders been requested? Have any protective orders been granted?

Answer: Protective orders under 8 C.F.R. 1003.46 have been requested 14 times. Thirteen orders have been issued.

d. If a protective order is granted, do the alien and the alien's counsel get access to the protected information?

Answer: Subject to the terms of the order, the respondent and respondent's counsel may receive the evidence that is the subject of the order.

e. Can the alien challenge the admissibility of the evidence that is protected by such an order?

Answer: A protective order does not alter the evidentiary standards that are applicable to the document being protected, and a respondent may challenge the admissibility of that evidence.

f. Do Federal court judges have a similar ability to issue protective orders to prevent the dissemination of information introduced in Federal court?

Answer: The United States District Courts use similar procedures under Federal Rule of Civil Procedure No. 26(c).

g. Can a government attorney be sanctioned for disclosing information in violation of an immigration judge's protective order?

Answer: Yes. An attorney for the government may be sanctioned for violating an immigration judge's protective order.

5. Section 411 of the USA PATRIOT Act amended the Immigration and Nationality Act to broaden the scope of aliens ineligible for admission or deportable due to terrorist activities. In its May 13, 2003 response to Committee questions on USA PATRIOT Act implementation, the Department stated that: "Prior to the transfer of the INS to DHS, the INS had not relied upon the definitions in section 411 to file new charges against aliens in removal proceedings."

a. Does this mean that the Justice Department has not concluded that any of the aliens with whom it has dealt since the passage of the USA PATRIOT Act in October 2001 were terrorists? If not, why weren't these aliens charged under these provisions?

Answer: The fact that an illegal alien was prosecuted for non-terrorist crimes or deported based on non-terrorism-related grounds of removal rather than prosecuted, does not mean that the alien had no knowledge of or connection to terrorism. For example, one immigration detainee who pled guilty to the non-terrorism-specific crimes of conspiracy to commit identification fraud and aiding and abetting the unlawful production of identification documents traveled overnight with two of the hijackers. Often in terrorism-related cases, an individual is deported or criminally charged on grounds seemingly unrelated to terrorism because the assertion of specific terrorism charges can compromise sensitive intelligence matters such as the sources and methods used to gather information.

In addition, in immigration proceedings, as opposed to the criminal context, the government is seeking only one remedy, removal. Therefore, the Department believes that the best use of resources is to seek removal of an alien based on the charge that is most likely to prevail and simplest to prove, such as a violation for overstaying one's authorized period of admission to the United States. Bringing terrorism-related grounds of removal against an alien can raise issues such as the use of classified information as well as the expectation that terrorism-related charges are more likely to bring federal court challenges which ultimately delay the removal of the alien and cost the American taxpayers money. In addition, in the immigration context, aliens in removal proceedings may utilize the fact that they have been charged with a terrorism-related ground of removal as a basis for an asylum claim, further delaying their successful deportation.

b. Have any aliens been charged with any terrorism-based ground of removal since September 11, 2001? If so, are these the only aliens with terrorist ties who have come to the attention of the Justice Department since September 11, 2001?

Answer: According to the records of the Executive Office for Immigration Review, four aliens were charged with terrorism-based grounds of removal between September 11, 2001, and March 1, 2003, when responsibility for bringing charges against an alien in immigration proceedings was transferred to the Department of Homeland Security. No alien who had been investigated in connection with the events of September 11th, and who had been placed in an immigration proceeding, was charged with terrorism-based grounds of removal or inadmissibility. We respectfully refer you to the Department of Homeland Security if you require further information in this connection.

c. Are there reasons that the Justice Department or INS would not have charged an alien believed to have a connection to a terrorist group or terrorist acts with a terrorism-related ground of removal? If so, why?

Answer: Please see response to 5(a), above.

d. How many aliens have been charged on terrorism-related criminal grounds since September 11, 2001? Are these the only aliens whom the Justice Department believes are related to terrorism?

Answer: Since September 11, 2001, six aliens have been charged with terrorism-related criminal grounds in connection with the PENTBOMB investigation. Similar to the response to questions (a) and (c) above, there may be many reasons why the Department has not brought criminal charges against individuals whom we believe to be connected to terrorism. For example, the information we possess may not relate to a specific criminal violation under U.S. law, or the information may be classified and cannot be declassified. In addition, the burden of proof is higher for criminal cases, and the information that we possess may not be sufficient to prove guilt beyond a reasonable doubt.

e. **Are there any reasons why the Justice Department would deport an alien who is suspected of terrorist ties or of engaging in terrorist activities rather than charging the alien criminally? Why would the Justice Department do this? Has the Justice Department done this?**

Answer: In some cases, the FBI and other law enforcement agencies were able to determine that aliens detained in connection with the September 11th investigation were no longer of investigatory interest and those individuals were subsequently released or deported. In other cases, while there may have been information linking an individual to criminal or terrorist activity, the information was not substantial enough to prosecute and all indications were that no further substantive information would surface. In those cases, in the interest of national security, it was determined that the best course of action was to proceed with deportation and remove a potentially dangerous person from our borders based upon an immigration violation rather than release the individual into American society. The Department believes that it is best advised to use all legal tools at our disposal to detain, investigate and prosecute violations of our nation's laws and ensure that any threats to the American people are neutralized, whether it be through detention or removal.

6. **The Department of Justice took a major step in tightening border security after September 11 by implementing the National Security Entry-Exit Registration System (or NSEERS), which required aliens to be fingerprinted, photographed and registered, both at the ports of entry and domestically. While control over this initiative passed to the Department of Homeland Security, what results do we have to show for this effort? Have any aliens linked to terrorism been identified through NSEERS? If so, how many? And have any criminal aliens been arrested through NSEERS?**

Answer: On June 13, 2002, the Department published a proposed rule to modify the regulations to require certain nonimmigrant aliens to make specific reports to the Immigration and Naturalization Service: upon arrival; approximately 30 days after arrival; every twelve months after arrival; upon certain events, such as a change of address, employment, or school; and at the time they leave the United States. 67 FR 40581. The Department adopted a final rule on August 12, 2002. 67 FR 52584. This program was known as the National Security Entry - Exit Registration System. This system, along with other functions of the former Immigration and Naturalization Service, transferred to the Department of Homeland Security on March 1, 2003, pursuant to the Homeland Security Act of 2002.

The Attorney General established NSEERS both as a direct means of protecting the United States from terrorism and to implement Congress' demands for a complete entry-exit management system. Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Div. C, § 110, Pub. L. No. 104-208, 110 Stat. 3009-558 (Sept. 30, 1996); Immigration and Naturalization Service Data Management Improvement Act of 2000, § 3, Pub. L. 106-215, 114 Stat. 337 (June

15, 2000); United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, tit. IV, subtit. B, § 414(b), Pub. L. 107-56, 115 Stat. 272, 353-354 (Oct. 26, 2001); Enhanced Border Security and Visa Entry Reform Act of 2002, tit. III, §302, Pub. L. 107-173, 116 Stat. 543, 552 (May 14, 2002).

In the brief period before the program transferred to the Department of Homeland Security, the Department found that over 3,000 aliens encountered through NSEERS were in violation of the Immigration and Nationality Act and warranted removal, and 28 aliens were the subjects of outstanding federal or state criminal arrest warrants. As of June 3, 2003, NSEERS had led to the identification of 11 suspected terrorists. In addition, INS/DHS had apprehended or denied admission at ports of entry to 766 aliens who presented law enforcement threats due to felony warrants or prior criminal or immigration violations, rendering them inadmissible. Moreover, the domestic registration of persons already in the United States enabled immigration officials to apprehend 136 felons who were in the country illegally. These included criminals guilty of homicide, aggravated assault against a law enforcement officer, sexual battery, assault with a deadly weapon, and cocaine trafficking.

The Department of Homeland Security has continued to implement the comprehensive entry-exit program begun by the Attorney General in NSEERS through the US VISIT program. With the US VISIT program beginning to stand up, it has been possible for the Department of Homeland Security to scale back specific requirements of the NSEERS program. We recommend that the Committee contact the Department of Homeland Security for more detailed and up-to-date information.

7. How does the Civil Rights Division and the U. S. Attorney's office coordinate with local prosecutors in instances where civil rights cases are being prosecuted locally?

Answer: As a general proposition, where state or local prosecutors are proceeding with a potential criminal civil rights case, we monitor the state and local effort. At the conclusion of the state court prosecution, we review the evidence, including the local police reports and any state court transcripts, to determine if federal interests have been vindicated by the state prosecution. In short, we work with State and local prosecutors to coordinate our investigations and charging decisions and to ensure that resources are expended wisely.

8. It is widely acknowledged that our nation's critical infrastructure is vulnerable to terrorist attacks. While we work to secure our airports, highways, and power plants, we must also ensure cyberspace is protected.

a. Are we prepared to deal with the possibility of a cyber attack?

Answer: The FBI is in a position to address the possibility of a cyber attack. We work closely with the Intelligence Community, Law Enforcement Agencies, other government agencies, and the private sector to collect intelligence and investigate computer intrusion matters, also known as cyber attacks. The FBI is the lead agency for these investigations when terrorists or nation-states are responsible for the intrusions. The Cyber Division is working closely with the House and Senate Appropriations Committees to ensure that the transfer of Cyber Division assets to the Department of Homeland Security does not impact on our ability to address computer intrusions. The FBI has launched an extensive recruiting effort to ensure that we have properly trained investigators working on these cases.

In addition, the FBI has regional squads across the country whose sole mission is to collect intelligence and investigate computer intrusion matters. In FY 2003, the FBI funded the creation of approximately 45 task force operations which will also investigate computer intrusion matters as part of their overall investigative responsibilities.

The FBI no longer includes the National Infrastructure Protection Center (NIPC), whose mission was to provide "a national focal point for gathering information on threats to the infrastructures" and to provide "the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts." The functions of the NIPC, excluding computer intrusion investigations, were transferred to the Department of Homeland Security by Pub. L. No. 107-296 (November 25, 2002).

b. Have you increased the level of prosecution for cyber crimes? If not, why? If so, can you quantify any decrease in the amount of cyber crime committed against interests in the United States?

Answer: The Department has moved aggressively to increase the number of computer crime cases prosecuted. As a result of increased Congressional funding over the past several years, the Department has added additional prosecutors focused on computer hacking and intellectual property crimes to eleven United States Attorneys' Offices around the country in regions with dense high-tech industry. Similarly, the Computer Crime and Intellectual Property Section in the Department's Criminal Division has added more prosecutors and has sought to bring more prosecutions in addition to its traditional role of supporting computer crime prosecutors in the field. For more information about recent computer crime prosecutions across the country, see http://www.cybercrime.gov/cccases.html.

Despite these increases, however, it is very difficult to correlate our prosecutorial efforts with the amount of computer crime that occurs in the United States. This difficulty results from two factors: (a) as the use of the Internet and society's dependence on computer networks continues to rise, these networks become increasingly attractive targets for criminals and terrorists; and (b) there has been a lack of comprehensive, reliable data from which to detect trends. Regarding the latter factor, investigation and prosecution of computer intrusions have historically suffered from

low levels of victim reporting, and to date, there have been few comprehensive studies of the amount of computer crime. Last year, however, the Bureau of Justice Statistics began a project to compile comprehensive and reliable statistics in order to understand the nature and scope of the threat of computer crime and better assess the impact of the Department's prosecutorial efforts.

9. **Press reports indicate that there may be a disagreement, or at the least, a debate within the government as how to proceed with the prosecution of Zacarias Moussaoui, now awaiting trial in federal court in the Eastern District of Virginia. The prosecution seems to be subject to an inordinate delay and it appears that the federal judge presiding in that case has questioned whether a federal criminal court is the appropriate forum. The *Washington Post* has characterized recently released court documents as revealing "a government and court system uncertain how to proceed against Moussaoui in a civilian court while trying to conduct an international war on terrorism and maintain national security." The judge reportedly has indicated that the Department of Justice's decision to try Mr. Moussaoui in a federal criminal court carried with it legal consequences and responsibilities.**

   a. **Were the legal consequences and responsibilities of trying this matter in a federal criminal court contemplated?**

Answer: Yes. The Department was well aware of its responsibilities under the Constitution, the law and the rules of procedure to ensure that justice is done, classified information is protected, and the defendant receives a fair, public, and speedy trial. The Department has honored those responsibilities and will continue to do so.

   b. **Are you satisfied that a civilian court, and that one located in the Eastern District of Virginia, is the appropriate place to prosecute Mr. Moussaoui and, if so, are you satisfied with the progress of that case?**

Answer: Yes, we are satisfied that a civilian court, and especially the one located in the Eastern District of Virginia, is the appropriate place to prosecute Mr. Moussaoui. The Eastern District of Virginia is well-known for its efficient handling of criminal cases, and the Department has been satisfied with the progress of this extremely complex case to date. The Department suggested an early trial date and has done all it can, consistent with the need to protect classified national security information, to bring the case to trial as soon as possible.

   c. **If that prosecution continues, can you predict when an actual trial is likely to begin or do you foresee continuing pre-trial motions, rulings and appeals which will further delay the matter?**

Answer: As you know, the government is currently appealing a critical national security issue regarding the district court's orders directing the government to allow Moussaoui to depose certain enemy combatants abroad. We hope to prevail in that appeal, which was argued before the Fourth Circuit on December 3, 2003, by Deputy Solicitor General Paul Clement. The case was taken under advisement, and a decision is expected in the near future. At this point it is not possible to predict whether defense counsel will file motions or the district court issue additional rulings that might necessitate the government taking an additional appeal to protect national security or other critical government interests, or whether the defense might attempt an appeal. We have and will continue to work to bring the case expeditiously to trial, and we have confidence the trial court will manage it toward that end. For example, in response to a motion from defense counsel for guidance on the setting of a trial date, the district court issued an order on November 5, 2003, in which, in addition to staying all proceedings in the trial court pending the appeal, the court ruled that no trial date will be set sooner than 180 days after return of the mandate, if the case remains a capital prosecution, or 90 days after the return of the mandate, if the sanctions imposed by the district court (and subject of the appeal) are upheld (i.e., if the case is not a capital prosecution). The district court also issued an order on November 14, 2003, vacating its prior decision allowing Moussaoui to represent himself. The defendant is now represented by able counsel, which should lead to more efficient progress of the case.

10. During the 107th Congress, the House of Representatives passed the Federal Agency Protection of Privacy Act (FAPPA) requiring federal agencies to include a privacy impact analysis to be commented upon by the public when issuing regulations.

a. In a time when the threat of terrorism has caused the government to take unprecedented actions that understandably impact upon traditional spheres of personal privacy, would it not allay many citizen concerns about government intrusion and overreaching if new regulations were drafted with an articulated consideration of those citizen concerns?

b. Can we anticipate the support of the Department of Justice for legislation, such as FAPPA, which follows a reasonable approach and takes moderate steps to insure federal regulations consider legitimate privacy concerns?

Answer: We are studying the issues raised by this proposed legislation; however, we are unable to provide a position at this time. We are committed however, to acting "reasonably" to insure that federal regulations take into account legitimate privacy concerns.

11. Does the Justice Department, any agent of the Department, or contractor on behalf of the Department investigate or maintain files on people who are not legitimate suspects of crime or terrorism?

Answer: Yes. The Department of Justice maintains a variety of investigative and background files on individuals who are not currently "legitimate suspects of crime or terrorism." Examples of such persons or entities would include: employees of the Department or applicants for employment (e.g., the results of background checks); contractors and bidders; grant applicants and recipients; material witnesses; civil litigants; foreign agents; persons entered into the National Crime Information Center; and others, consistent with the Department's lawful responsibilities. This list is not intended to be exclusive.

12. You may recall that I asked you during the June 5th hearing to comment on whether you were aware of any data-mining efforts by any component within the Justice Department that collects information on individuals other than criminal suspects. As a follow-up to that query, I mentioned that I may want you to respond in writing.

a. Accordingly, would you please provide your written response?

Answer: As noted in our answer to question 11, consistent with the Department's lawful mission, we regularly collect and maintain files and information on a variety of persons who are not the suspects of crime or terrorism. "Data mining" -- the collection of related information from electronic sources -- is performed in connection with legitimate, lawful activities of the Department. For example, it would not be uncommon for a person who applies for employment with the Department, and who is otherwise a public figure, to be the subject of a "Google" search on the Internet in the course of the mandatory background investigation.

b. In addition, are you aware of any agent of the Department or contractor on behalf of the Department that collects information on individuals other than criminal suspects?

Answer: See the response to question 11.

c. Does the Department investigate or maintain files on people who are not legitimate suspects of crime or terrorism?

Answer: See the response to question 11.

13. What were the data sources used to identify the detainees rounded up following the September 11, 2001 attacks?

Answer: Immediately following the September 11, 2001, attacks, the FBI received leads from various sources, including telephone calls from concerned individuals to FBI field offices, information from other agencies, tips from our established sources and assets, calls to our 1-800 hotline numbers, and information obtained through our full and preliminary investigations. In

following these leads, if FBI Agents or other JTTF members discovered that subjects were "out of status," the INS was notified so that they could pursue arrest or other appropriate action based on this immigration status.

14. On May 31, a *Philadelphia Inquirer* editorial made the following observations:

Why, for instance, have so many criminal cases been mislabeled as instances of international terrorism? As Inquirer staff writer Mark Fazlollah has documented, dozens and dozens of people charged in such cases have proven to be unconnected to terror groups. Could someone be trying to hype the antiterrorism benefits of the new powers to build a case to extend them even further?

In New Jersey, federal prosecutors recently pulled 65 Middle Eastern students' cases from terrorism lists. They said the students' hiring of stand-ins to take English exams for college was not terrorism-related.

What is your response?

Answer: The allegation that the Department is intentionally mislabeling numerous terrorism-related matters is not accurate. The information cited in this editorial appears to be based on a January 2003 report by the General Accounting Office (GAO) that cited 288 terrorism-related cases as being "misclassified". The problem cited by the GAO report was caused not by intentional mislabeling, but by transition issues resulting from a change in how anti-terrorism cases were categorized prior to September 11th and how they are subsequently categorized after September 11th. The "misclassifications" were the result of late notice to the United States Attorneys' Offices of Terrorism and Anti-Terrorism code changes and insufficient time for offices to make the changes prior to the GAO report. The GAO report acknowledged the fact that 127 of the "misclassified" cases fell under new anti-terrorism case categories and that only five of the 288 cases the GAO cited, or less than two percent, were unrelated to terrorism or our anti-terrorism efforts.

These classification codes were revised and supplemented after September 11th to properly capture the types of prosecutions being used to fight terrorism. Prior to September 11th, the Executive Office for United States Attorneys (EOUSA) had only two terrorism-related case classification codes -- International Terrorism and Domestic Terrorism. Reflecting the new reality after September 11th, EOUSA first added a case classification code for Terrorism-Related Hoaxes, then later added a code for Terrorist Financing and several codes for Anti-Terrorism (such as Identify Theft, Immigration, and Violent Crime) to capture activity intended to prevent or disrupt potential or actual terrorist threats where the offense conduct would not fall within one of the already-existing codes.

Under the new codes, the broad range of prosecutions used to disrupt activities that could facilitate or enable future terrorist acts and anti-terrorism cases are now able to be captured.

While some of these illegal acts may prove to be for personal benefit, activities such as identity theft, and immigration violations may also be used to position individuals who plan to commit future acts of terrorism. So called "sleepers" are difficult to identify as they will seek to blend in with minimal illegal activity until they are activated.

To ensure that data on all anti-terrorism cases is captured and included in EOUSA statistics, EOUSA, working with the Department's Criminal Division, on August 7, 2002, sent a memorandum to all United States Attorneys directing that appropriate pending cases and appropriate cases closed in Fiscal Year 2002 be reclassified, if needed, to reflect the new case classification codes. Under this directive, all Terrorism/Anti-Terrorism cases in Fiscal Year 2002 should have been re-sorted according to the new codes. With the transition to a new coding scheme so close to the end of the fiscal year, some United States Attorneys' Offices either did not have time to, or did not fully understand the need to, reclassify already closed cases.

EOUSA has and will continue to take every reasonable step to ensure that proper reclassification is completed and that future data entries are complete and accurate. A process exists for the review of United States Attorney case management system data and EOUSA is working to continue to oversee and validate the accuracy of case classification and conviction data entered into the case tracking system by the various United States Attorneys' Offices. On April 9, 2003, EOUSA sent a directive to the United States Attorneys asking them to review all Terrorism and Anti-Terrorism matters and cases and ensure that the most appropriate Terrorism or Anti-Terrorism program category code is assigned. The United States Attorneys' Offices are required to perform this data quality review quarterly. This directive re-emphasized the critical role of the United States Attorneys in providing the Department with accurate and timely caseload data.

The Department is committed to accurate reporting and accountability for cases prosecuted in federal court. This reporting ensures, for example, that Congress is able to provide adequate oversight of the Department's activities, and ensure that the Department has adequate resources. To the extent that the GAO Report identified various weaknesses in the current system, the Department is committed to taking every reasonable step to ensure that proper reclassification is completed and that future data entries are complete and accurate.

Finally, the referenced cases in the District of New Jersey began as an investigation into a fraudulent scheme whereby people paid imposters to take the Test of English as a Foreign Language (TOEFL). During the course of the investigation, it was discovered that one of the test takers had in his possession material that caused the investigation to broaden. The investigation into possible terrorist activity was pursued vigorously and fortunately terrorist activity was not discovered. At the conclusion of the investigation, it would have been more appropriate for the cases to be coded under an Anti-Terrorism category.

15. What would be your reaction to legislation that required the Justice Department to provide the following information to Congress on an annual basis:

a. a public report on the total number of U.S. persons targeted for court orders under FISA and the number of persons targeted for electronic surveillance, physical searches, pen registers and business records; the names and identities of those targeted would not have to be revealed;

Answer: Public reports concerning investigative methods and techniques are problematic because they may provide information that assists subjects and potential subjects to evade investigative efforts by avoiding those vehicles that receive the greatest investigative attention and using those that receive the least. We believe that the FISA strikes an appropriate balance between public reporting and national security concerns by requiring full reporting, in a classified setting, to the Senate Select and House Permanent Select Committee on Intelligence on a semi-annual basis.

b. a public report on the number of times that information acquired through a FISA order is authorized for use by the Attorney General in criminal proceedings; and

Answer: The Department is required by the FISA, 50 U.S.C. § 1808, to submit a semiannual report to the House Permanent Select and the Senate Select Committees on Intelligence. These reports include information on the number of times that information acquired through a FISA order is authorized for use by the Attorney General in criminal proceedings. In addition, the Attorney General's authorization to use information obtained through a FISA order in civil or criminal litigation is frequently made public when the government gives notice of its intent to use that information in the litigation or when the information is introduced in court. Because this information is already subject to congressional oversight and is publicly disclosed on appropriate occasions, the Department would not support further public release of this information.

c. a report to the House and Senate Judiciary Committees on surveillance of public and university libraries?

Answer: As noted above, public reports may allow foreign terrorists and spies to modify behaviors to take advantage of lesser used investigative methods and techniques. In addition, a reported increase in the use of these techniques may alert foreign terrorists and spies to the likelihood of their surveillance, causing them to change their methods or locations to avoid future detection.

16. I think that there are two ways to look at the Fourth Amendment of the Constitution from a law enforcement perspective. One view gives it an interpretation favoring efficiency over personal protection. In other words, giving law enforcement the benefit of the doubt. The other views it as an ideal embodying traditional preservation of individual privacy rights that mandates the inefficiency of search and seizure for the sake of maintaining those rights.

Which view point is yours and how have you specifically implemented that philosophy within the Department?

Answer: First and foremost, the Fourth Amendment safeguards the privacy of the American people and the inviolability of their property, specifically protecting "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." We agree with the U.S. Supreme Court that the "touchstone of the Fourth Amendment is reasonableness." *United States v. Knights*, 534 U.S. 112, 118 (2001). Specifically, the reasonability of a search under the Fourth Amendment is determined "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999). The provision thus generally calls for balancing an individual's interest in privacy with the legitimate needs of law enforcement. The Department of Justice is sensitive to the fact that important factors weigh on both sides of this balance, and, in all of its law enforcement activities, the Department zealously attempts to conform its conduct to applicable Fourth Amendment jurisprudence.

17. **Terrorism Investigations and Use of Statutory Authority**

Prior to enactment of the USA PATRIOT Act, the evidentiary standard for a FISA order for business records was relevance and "specific and articulable facts" giving "reason to believe" that the person to whom the records related was an agent of a foreign power. The PATRIOT Act dropped the additional requirement that there be "specific and articulable facts giving reason to believe" that the person to whom the records related was an agent of a foreign power. So these records simply need to be relevant to a terrorism investigation.

a. **Does this permit the Department to obtain the business records of a person who is not an agent of a foreign power but is the target of a terrorism investigation?**

b. **Does this also apply to a U.S. person who is the target of the investigation?**

c. **Does this also apply to an American citizen who is the target of the investigation?**

d. **Can the Department obtain the business records of a person who is not an agent of a foreign power nor the target of a terrorism investigation if it is determined that the records sought are relevant to such an investigation?**

e. **Does this also apply to a U.S. person who is not an agent of a foreign power nor the target of a terrorism investigation?**

f. Does this also apply to an American citizen who is not an agent of a foreign power nor the target of a terrorism investigation?

Answer:

50 U.S.C. § 1861(a)(1) authorizes the FBI to seek a court order "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." Such an investigation of a United States person may not be "conducted solely upon the basis of activities protected by the first amendment to the Constitution." Similarly, 50 U.S.C. § 1861(b)(2) requires that applications for the production of business records "specify that the records concerned are sought for an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."

There is no requirement in § 1861 that the party upon whom the order is served be an agent of a foreign power or the target of an international terrorism investigation or an investigation to protect against clandestine intelligence activities, so long as the records sought are for an appropriate investigation. This is so regardless of whether the recipient of the order is a non-U.S. person, a U.S. person, or a U.S. citizen. Indeed, it will be the unusual case in which a § 1861 order is served on someone who is the subject of an investigation because doing so would obviously alert the subject to the existence of the investigation, something the FBI is generally unlikely to desire.

The more likely scenario is that § 1861 orders will be directed at third parties who are in possession of documents that are relevant to the investigation of someone else. For example, if the FBI is seeking employment records regarding a suspected terrorist, the § 1861 order will be served upon the employer of the suspected terrorist, not the suspected terrorist himself. The order would be served on the employer (who is not an agent of a foreign power nor the subject of an investigation) and would seek records belonging to the employer that are about the suspected terrorist, but would not be records that belong to the suspect. A similar example would be hotel records that contain information about a visit by a suspected terrorist. The records belong to the hotel, not the suspect, and the hotel is unlikely to be an agent of a foreign power or a suspect of the investigation.

In addition, there may be circumstances in which the FBI seeks records pertaining to an individual who is neither an agent of a foreign power nor the subject of an appropriate investigation where the information nevertheless is for an ongoing investigation. For example, if there is reliable information that one or more terrorists whose identities are unknown are traveling on a particular flight on Acme Airlines, a § 1861 order served on Acme Airlines for a

list of all passengers on the flight would be appropriate, even though many individuals on the flight undoubtedly are innocent.

In reviewing the examples set forth above, it is important to remember that such information has, for many years, been available to the Government through Federal grand jury subpoenas without prior judicial review. By contrast, § 1861 requires prior court approval before the Government can obtain such records.

18. During your testimony, there was some confusion about the scope of Section 215 of the USA PATRIOT Act. Please clarify which types of records could be obtained under Section 215.

a. Does that include:

Book purchase records?
Library records of materials checked out?
Computer records?
Medical records?
Pharmaceutical records?
Educational records?
Firearm purchase records?
Membership lists from a club or association?
Membership lists from a religious institution?
Membership information (e.g. payments, services used, etc...)?
Tax records held by a tax preparer?
Political contributions?
Genetic information?

b. Has the Department used Section 215 authority to obtain:

Library records of materials checked out?
Computer records?
Medical records?
Pharmaceutical records?
Educational records?
Firearm purchase records?
Membership lists from a club or association?
Membership lists from a religious institution?
Membership information (e.g. payments, services used, etc...)?
Tax records held by a tax preparer?
Political contributions?
Genetic information?

c. Could the Department request an entire database of a business, association, religious institution or library under Section 215?

Answer: Section 215 of the USA PATRIOT Act allows the FISC, in terrorism and other national-security investigations, to order the production of business records - similar to the way that grand juries may subpoena the same sorts of records in investigations of ordinary crimes. Under section 215, the FISC is authorized to issue an order requiring the production of "any tangible things." 50 U.S.C. § 1861(a)(1). This language is identical to Fed. R. Civ. P. 34(a), which allows parties during discovery to demand the production of "any tangible things" in the possession of another party. In fact, section 215 contains a number of unique safeguards and limitations that have no counterpart in the grand jury context. For instance, section 215 requires that a federal court explicitly order the production of business records; by contrast, a grand-jury subpoena typically is issued without any prior judicial review or approval. Additionally, in investigations of U.S. persons, section 215 can be used only to protect against international terrorism or clandestine intelligence activities; a grand jury can obtain business records in investigations of *any* federal crimes. Further, section 215 expressly protects First Amendment rights; the grand-jury authorities contain no such protections. The section 215 order must also be consistent with other provisions of Federal law.

The Department of Justice is required every six months to "fully inform" Congress "concerning all requests for the production of tangible things under section 1861 of this title." 50 U.S.C. § 1862(a). The most recent report was delivered to the House Permanent Select and the Senate Select Committees on Intelligence and the House and Senate Committees on the Judiciary on January 5, 2004. On September 18, 2003, the Attorney General declassified the number of times to date the Department of Justice, including the Federal Bureau of Investigation (FBI), had utilized Section 215 of the USA PATRIOT Act relating to the production of business records. At that time, the number of times Section 215 was used was zero.

19. In his July 26, 2002 letter to the Judiciary Committee, then-Assistant Attorney General Daniel J. Bryant stated, in regard to Section 215, that "Under the old language, the FISA Court would issue an order compelling the production of certain defined categories of business records upon a showing of relevance and "specific and articulable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power. The PATRIOT Act changed the standard to simple relevance" (emphasis added). On numerous occasions in statements to the news media, DOJ spokespersons have stated that in order to examine someone's library records or book purchase records they must be an agent of a foreign power. As recently as May 22, 2003, the Associated Press reported that according to DOJ spokesman Jorge Martinez "the law only gives agents the power to research the library habits of 'agents of a foreign power' and won't be used to investigate 'garden-variety crimes'..."We're not going after the average American, we're just going after the bad guy."---"Library Privacy; Librarians find ways around USA PATRIOT Act" by Allison Schlesinger of the Associated Press. DOJ spokesman

Mark Corallo was quoted in the *Bangor Daily News* on April 4, 2003 saying that critics of Section 215 were "misleading the public" and that "the fact is the FBI can't get your records." It appears these statements are not true.

a. Why are your spokespersons providing conflicting information about this law?

b. What steps are you and the Department taking to ensure that accurate information is disseminated to our citizens?

Answer: We regret any confusion that has arisen in this area. As Assistant Attorney General Bryant's letter of July 26, 2002, to the Judiciary Committee noted, under section 215 of the USA PATRIOT Act, the standard for issuance of a FISA order was changed from "'specific and articulable facts' giving reason to believe that the person to whom the records related was an agent of a foreign power," to a simpler "relevance" test. For additional information regarding the nature of the information required to obtain a FISA order under the USA PATRIOT Act, please refer to the answers to question 17.

The Department's efforts have been directed at correcting the inaccurate and misleading statements about section 215 of the USA PATRIOT Act – including the erroneous claim that the FBI can gain access to business records without a court order. Under section 215, the FBI cannot unilaterally get business records (including library records). Rather, this authority allows the Justice Department to seek such records only pursuant to an order issued by the FISC. Such orders are available only in a narrow set of investigations: (1) to obtain foreign-intelligence information about people who are neither American citizens nor lawful permanent residents; or (2) to defend the United States against spies or international terrorists. Section 215 cannot be used to investigate garden-variety crimes, or even domestic terrorism.

20. Section 215 does not allow an investigation of a U.S. person if such an investigation is conducted "solely upon the basis of activities protected by the First Amendment to the Constitution."

a. Would this limitation still allow an investigation based in part on activities protected by the First Amendment?

Answer: Under Executive Order 12333, the FBI is one of the government agencies that is authorized to conduct investigations to collect "accurate and timely information about the capabilities, intentions and activities of foreign powers, organizations, or persons and their agents" for the purpose of the "acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers." E.O. 12333, parts 2.1 and 2.2. All agencies covered by E.O. 12333 are to conduct their activities, including investigations, in a manner that "achieves the proper balance between the acquisition of essential information and protecting of individual interests." E.O. 12333, part 2.2.

These provisions anticipate that many investigations identify a variety of activities undertaken by the target of the investigation that may include some activity deemed protected by the First Amendment, such as the identities of the persons or institutions with whom the target has associated or where the target has traveled. These facts could be part of the entire set of facts and circumstances taken into consideration in determining whether an investigation is warranted for the purpose of acquiring significant foreign intelligence, or detecting and countering international terrorist activities or espionage.

b. What definition of "activities protected by the First Amendment" is used by the department in evaluating a request for a FISA order?

Answer: In determining whether "activities are protected by the First Amendment," as that phrase is used in 50 U.S.C. §§ 1861(a)(1) & (2)(B), the Department consults the First Amendment jurisprudence of the U.S. Supreme Court as well as other federal courts.

c. What procedures are in place to ensure that such orders are not sought solely on the basis of activities protected by the First Amendment of the U.S. Constitution?

Answer: In preparing an application for any FISA order, including any application under section 215, the Office of Intelligence Policy and Review of the Department of Justice conducts a review to determine that the underlying investigation is not being conducted solely on the basis of those constitutionally protected activities. An application that did not contain such other facts and circumstances would not be presented to the Foreign Intelligence Surveillance Court for approval.

21. DOJ spokesman Mark Corallo has been quoted as saying that the Department is considering holding public hearings around the country to explain and debate the USA PATRIOT Act (*Bangor Daily News*, April 4).

a. Will the Department conduct a series of public hearings around the country on this topic?

Answer: Last year, Mr. Corallo discussed the possibility of a more formal response to the campaign of misinformation by opponents of the Patriot Act. This past summer, the Attorney General visited over 30 cities across the country to discuss the USA PATRIOT Act and the government's efforts in the war on terrorism. The Attorney General spoke to members of the law enforcement community and conducted over 100 media interviews -- television, radio, and print -- in order to educate the public about the Patriot Act. Simultaneously, the United States Attorneys across the country held dozens of town-hall meetings to inform the citizens of their communities about the Act and answer any questions posed by the public.

b. If so, will you make available high ranking DOJ officials to participate in these hearings to listen directly to the public?

Answer: See answer to 21(a) above.

c. Will you provide other opportunities for the public to give input and feedback about changes to our criminal and foreign intelligence investigation laws and guidelines made since September 11, 2001 with the stated purpose of assisting in the war on terrorism?

Answer: It would be appropriate for the Congress to entertain public comments about any changes in the laws. The Justice Department will continue to enforce the laws passed by Congress and defend the American people from terrorist attacks.

22. As you know, a draft of the so-called PATRIOT Act II has been circulating in the media and on the web for several months. I accept your testimony that you are not planning to introduce it now or in the future in its current form. However, as you know, the USA PATRIOT Act was rushed through Congress with little time for the kind of extensive debate typically given to such a proposal. We can debate the need for moving it so quickly at that time, but I think we can agree that it was a very significant expansion of prosecutorial and investigative authority.

a. Will you promise to engage in a full and complete debate over any additional powers or authorities that you request in the future?

b. Can we have your personal assurance that you and the Department will not try to pressure the Congress, directly or through the media, to act on requests for expanded authority prior to a full and complete debate?

Answer: The Department of Justice is fully committed to consulting with Congress on all legislative initiatives, including those designed to protect the American people from terrorist attacks while preserving their civil rights and liberties. All branches of the federal government have a vital part to play in the war on terrorism, and Congress's role in the development and adoption of anti-terrorism legislation is a significant one indeed.

In many ways, the extensive consultations and deliberations that characterized the adoption of the USA PATRIOT Act are the model of effective interbranch cooperation. In the six weeks between the terrorist attacks of September 11 and October 26, 2001, when the President signed the USA PATRIOT Act into law, high-ranking Executive Branch officials met with Members of Congress and their staffs on countless occasions to discuss the legislative response to the attacks of September 11th. These intensive discussions resulted in the USA PATRIOT Act being passed in the Senate by a near-unanimous margin of 98-1, and 357-66 in the House of Representatives,

with the support of members from across the political spectrum. We anticipate that, should any anti-terrorism legislative proposals be introduced in the future, those measures would inspire similarly extensive consultations and deliberations.

23. The USA PATRIOT Act made numerous changes that enhanced the power of the federal government to investigate and prosecute terrorism threats and crimes. Some of these powers apply only to terrorism investigations, while others are tools that apply to all federal investigations. Now that you have had time to use many of these tools, it would be very helpful to our oversight efforts to know which ones the Department finds most valuable and useful and which ones are less important, not used frequently, or unnecessary.

a. Can you tell us which authorities have proved most useful and why?

Answer: Although prior to the signing of the USA PATRIOT Act, there were criminal statutes that addressed the investigation and prosecution of terrorism threats and crimes, they were not sufficient to combat the complexity nor the severity of modern terrorism. Limitations on jurisdiction and a lack of legal tools to deal with emerging terrorist techniques prevented the U.S. government from sufficiently tackling the serious threat of terrorism in the modern world. The USA PATRIOT Act addressed this problem by both applying current statutes (e.g., the RICO statutes) to terrorism and also developing new statutes, e.g. sections 201, 801, 810, specific to modern terrorism. These innovations have been critical in the fight against terrorism. Federal prosecutors and United States Attorneys have already employed many of these new tools in several cases as well as ongoing investigations. The following provides a more detailed explanation of specific sections of the USA PATRIOT Act and their application. This list is by no means complete as there are numerous sections which have been used or are currently being used in ongoing investigations. Rather, we have tried to provide a broad sampling of the ways in which the PATRIOT Act has been used to illustrate its utility and necessity.

The USA PATRIOT Act has enabled the U.S. government to more effectively process and analyze law enforcement and intelligence information. Prior to the Act, intelligence and law enforcement agencies and personnel were discouraged from sharing certain types of information. This restriction represented a serious impediment to effective antiterrorism efforts and risked unproductive approaches to the apprehension and prosecution of terrorists and criminals. Provisions of the Act, such as sections 203, 218, 403, 504, and 905, have enabled the intelligence arm and the law enforcement arm of the U.S. government to coordinate their efforts by breaking down the "wall"[1]. As FBI Director Robert Mueller explained, "[t]he Patriot Act has allowed us

[1]Section 203 allows for the sharing of information between the intelligence and law enforcement communities.
Section 218 amends the predicate for the use of the Federal Intelligence Surveillance Act (FISA) to a "significant" purpose of foreign intelligence.

to ensure that the aggregate intelligence gleaned from those cases is analyzed for trends and for connections that might not be visible to us from a review of individual cases. This threat-based look at FBI intelligence has allowed us to uncover terrorist networks and connections within the United States that otherwise might not have been found."[2]

Such exchanges of information have occurred between the law enforcement and intelligence communities on numerous occasions. Sections 218 and 504 were essential to the success of the Sami Al-Arian investigation in Tampa, Florida. Al-Arian was indicted on conspiracy charges related to his involvement with the North American cell of the Palestinian Islamic Jihad (PIJ) cell. Sections 218 and 504 enabled prosecutors to consider all evidence against the defendant, Sami Al-Arian, including evidence obtained pursuant to FISA. By considering the intelligence and law enforcement information together, prosecutors were able to create a complete history for the case and put each piece of evidence in its proper context. This comprehensive approach enabled prosecutors to build their case and pursue the proper charges. Thus, sections 218 and 504 were essential in allowing prosecutors to fully consider all evidence in this particular case and then move forward in an appropriate manner.

Information exchange under sections 203 and 905 has occurred via FBI JTTFs. The number of Joint Terrorism Task Forces has nearly doubled since September 11th, and the staff has greatly increased. These task forces have been integral to the dissemination of information between agencies, which has resulted in actual convictions. The information-sharing proscribed by section 403 has also yielded significant results. The FBI has already turned over more than 8.4 million records from NCIC databases to the State Department and disclosed 83,000 comprehensive records of key wanted persons from the NCIC databases to the INS.

In addition, the USA PATRIOT Act has improved law enforcement officers' ability to obtain critical evidence necessary to thwart terrorist plans and apprehend the terrorists themselves. The Department of Justice has found sections 207, 213, and 219 particularly useful in this regard[3].

Section 403 requires the FBI to share criminal-record information with the INS and the State Department for the purpose of adjudicating visa applications.
Section 504 allows for coordination between the intelligence community and the law enforcement community in FISA searches and surveillance.
Section 905 requires the Attorney General to disclose to the CIA Director any foreign intelligence acquired by a DOJ element during a criminal investigation; the Attorney General can provide exceptions for classes of information to protect ongoing investigations.

[2]Robert S. Mueller, "Combatting [sic] Terrorism" (congressional statement presented before the United States Senate Committee on the Judiciary, July 23, 2003).

[3] Section 207 increases the number of days for a search or surveillance order.
Section 213 provides for delayed notification warrants, especially in situations regarding public and officer safety.
Section 219 allows courts to approve nationwide search warrants in terrorist investigations.

Section 207 has afforded law enforcement officials the additional time needed to conduct intricate and complex terrorist investigations. It has also alleviated the burden of constantly reapplying for and adjudicating search warrant requests, time which could better be spent on the investigation and prosecution of the offenders.

Section 213 has been essential in increasing the safety of government officials and witnesses as well as the effectiveness of terrorist investigations. Advanced notification to terrorist suspects of searches or surveillances could result in destroyed evidence, notification of co-conspirators, attacks on agents and potential witnesses, or even the immediate execution of a terrorist plot. Between October 26, 2001, and the Spring of 2003, 47 delayed notice warrants had been issued. Those instances include cases which have since been charged, e.g. *United States v. Odeh*, a narco-terrorism case, and *United States v. Dhafir*, a money laundering case, and others still pending. Section 213 has enabled investigators to obtain decisive evidence for the prosecution of serious offenders.

Section 219 expedited the process for obtaining warrants in complex multi-district cases. This section has saved investigators valuable time by enabling the judge most familiar with a case to approve a request for a search warrant for premises outside his/her district. In connection with the anthrax found at America Media, Inc. in Boca Raton, Florida, federal investigators were permitted by section 219 to obtain a search warrant for those premises from the federal judge in Washington, D.C., presiding over the larger investigation who was knowledgeable regarding the entire investigation.

The USA PATRIOT Act refinements pertaining to communications have also significantly enhanced the tools available to investigators and prosecutors. The sections related to voice mail, the Internet, and computers were critical to the investigation of the Daniel Pearl case, which made use of sections 209, 212, 216, and 220 of the USA PATRIOT Act[4]. Not only were investigators able to compile important evidence in the case using these means but they were also able to identify some of the perpetrators.

These communication provisions have also been used in other federal cases. For example, under section 212, federal agents were able to obtain the identity of a person posting online bomb death threats directed at high school faculty and students. Similarly, section 216 aided a variety of

---

[4]Section 209 allows voice mail stored with a third party provider to be obtained with a search warrant, rather than a wiretap order.
Section 212 allows computer-service providers to disclose communications and records of communications to protect life and limb; and clarifies that victims of computer hacking can disclose non-content records to protect their rights and property.
Section 216 amends the pen register/trap and trace statute to apply to internet communications, and to allow for a single order valid across the country.
Section 220 permits courts to issue search warrants for communications stored by providers anywhere in the country; court must have jurisdiction over the offense.

federal investigations, including investigations of terrorist conspirators, a drug distributor, and a four-time murderer. Section 220 was used to follow a dangerous fugitive and a computer hacker who stole a company's trade secrets and then extorted money from the company.

Other sections which address new forms of technology and communication have also been utilized. Section 210 was used to combat computer hackers targeting over fifty government and military computers[5]. Section 217, which placed cyber-intruders on the same footing as physical intruders, has enabled hacking victims to seek law-enforcement assistance to combat hackers, just as burglary victims can invite police officers into their homes to catch burglars[6]. Since the passage of the USA PATRIOT Act, this provision has been used on several occasions.

Three sections of the USA PATRIOT Act have been particularly useful in money laundering investigations and prosecutions. They are Sections 319(a), 371 and 373.

Section 319(a), added a new subsection, 18 U.S.C. § 981(k), which provided the authority to forfeit funds in the U.S. correspondent account of a foreign bank where funds subject to forfeiture are deposited in a foreign bank account. While this authority has been used only where there is no other feasible alternative, such as where there is no treaty with the foreign country or where the foreign country is not cooperative, 18 U.S.C. § 981(k) has provided the basis for the seizure and forfeiture of funds in five cases involving a total of approximately $7 million.

To date, these cases have involved fraud schemes or illegal money transmitting violations under 18 U.S.C. § 1960, which was amended by Section 373 of the USA PATRIOT Act (see below). The Department first used Section 319(a) less than a month after Congress enacted the USA PATRIOT Act to seize $1.8 million in fraud proceeds deposited in a bank account in Belize. Because the Belizean bank maintained a correspondent account at a New York bank, the funds in the correspondent account were subject to seizure under Section 319(a). More recently, funds were seized from U.S. correspondent accounts following the deposit of criminal proceeds or funds transmitted in violation of 18 U.S.C. § 1960 in banks in Yemen, Oman, India, Taiwan, Israel, and Jordan.

Section 371, codified at 31 U.S.C. § 5332, prohibits smuggling currency or monetary instruments in an amount exceeding $10,000 across U.S. borders. Since its enactment, this authority has been used repeatedly to prosecute currency smugglers and to forfeit currency involved in the smuggling offense.

---

[5]Section 210 clarifies the types of records that law enforcement can subpoena from communications providers, including the means and source of payment.

[6]Section 217 enables victims of computer attackers to seek law enforcement officers' help in monitoring trespassers on their systems.

In Section 373, Congress amended 18 U.S.C. § 1960 to prohibit money transmitting businesses from operating without a state license or without being federally registered, and to prohibit the transmission of criminal proceeds or any funds transferred in support of criminal activity. The amended version of 18 U.S.C. § 1960 has been an extremely useful tool in the prosecution of money transmitting businesses who operate without licenses or who transmit funds in violation of its provisions. Among the successful prosecutions to date are *United States v. Mohamed Albanna* (W.D. N.Y.) and *United States v. Mulamin Turay* (W.D.KY). Most recently, in the Lakhani case in New Jersey, the Department of Justice charged two of the co-defendants with conspiracy to violate 18 U.S.C. 1960 when they allegedly accepted a $30,000 "downpayment" for shoulder-fired missiles in cash and remitted it through an unlicensed money transmitter to the supposed supplier.

Other highly useful provisions of the USA PATRIOT Act in money laundering prosecutions include Sections 322, 363, 365, 372 and 377.

Section 322 filled a loophole in the "fugitive disentitlement doctrine" enacted as part of the Civil Asset Forfeiture Reform Act of 2000 (Pub. L. No. 106-185). Through this provision, codified at 28 U.S.C. § 2466, fugitives in criminal cases are prevented from contesting the forfeiture of property in a related forfeiture case unless he or she returns to face the criminal charges. Section 322 made clear that a fugitive may not use a corporation to contest a forfeiture where the fugitive is a majority shareholder or is using the corporation to do indirectly what he or she could not directly.

Section 365 of the USA PATRIOT Act created a new provision requiring nonfinancial trade or businesses to report to the Financial Crimes Enforcement Center one or more related currency transactions exceeding $10,000. While this provision has been useful to prosecutors, a typographical error referring to a non-existent section has created unnecessary confusion regarding the ability to forfeit the proceeds of this criminal activity.

Also useful have been the new specified unlawful activities and RICO predicates added by Sections 315, 375 and 813, which amended 18 U.S.C. §§ 1956(c)(7) and 1961(1) to include corruption by foreign public officials, terrorist crimes, and other unlawful acts that generate proceeds. While the ex post facto clause of the U.S. Constitution has limited the full use of the new specified unlawful activities in criminal cases, some of the new provisions have been used in connection with civil forfeiture proceedings under 18 U.S.C. § 981.

In connection with forfeiture proceedings, the amendment to 21 U.S.C. § 853(e)(4) in Section 319 of the USA PATRIOT Act has provided important authority to order defendants in criminal cases to repatriate assets held outside U.S. borders. This provision is now embodied in the form of restraining orders that the Department of Justice provides for prosecutors to use in any criminal case in which it appears that the defendant may have placed forfeitable assets abroad.

In addition, Section 1004 of the USA PATRIOT Act, codified at 18 U.S.C. § 1956(i), clarified that venue was proper for a money laundering charge in the district where the underlying specified unlawful activity occurred, if the defendant participated in the transfer of the proceeds from that district to the district where the money laundering transaction occurred. Additionally, the new authority resolved a split in the Circuits by defining a transfer of funds as a single, continuing transaction. The new venue authority has facilitated money laundering prosecutions in virtually every district.

The USA PATRIOT Act also criminalized certain activities not specifically and clearly covered before. For example, section 803 made it a crime to harbor terrorists. Similarly, new sections on "material support" have enabled prosecutors to truly address the global nature of terrorism. Section 805 of the USA PATRIOT Act bolstered the ban on providing material support to terrorists by clearly making it a crime to provide terrorists with "expert advice or assistance," and by clarifying that "material support" includes all forms of money, not just hard currency. In addition, section 810 increased the penalty for providing material support to a terrorist organization from 10 to 15 years' imprisonment. For example, members of a terrorist cell in Buffalo were charged with and pled guilty to providing material support relying on these provisions.

Some of the sections of the USA PATRIOT Act have focused primarily on increasing government personnel and resources. Both the need for and benefit of this increased capacity are already evident. Prior to the passage of the USA PATRIOT Act, the United States was vulnerable to those who would use our programs for education and cultural exchange to enter the U.S. for other purposes. The U.S. government has always cherished the cultural exchanges it has hosted within its own borders. However, the government is also ever aware of its responsibility to safeguard our citizens as well as our lawful visitors. Post-9/11 we learned that one of our most serious threats can come from within the U.S. if we allow members of terrorist cells to enter and lay dormant, waiting for an opportunity to strike. With this in mind, the USA PATRIOT Act has increased immigration personnel and tools to ensure that those entering the U.S. are doing so with the intention of learning and contributing to the U.S., rather than seeking its destruction.

The northern border of the United States has long been seen as a potential entry point for terrorists as it was understaffed and insufficiently monitored. Section 402 tripled the number of Border Patrol personnel, Customs Service personnel, and Immigration and Naturalization Service inspectors. It also allocated an additional $50 million each to the Customs Service and the INS. An inability to efficiently track foreign visitors also posed a threat to national security. Section 414 required the U.S. government to quickly implement the exit and entry data system requested by the Congress in 1996. The INS has already completed the National Security Entry Exit Registration System (NSEERS). NSEERS, while not part of the PATRIOT Act, is able to both monitor entry into the United States as well as track expired visas or persons who have failed to fulfill the stated purpose of their reason for entry. As of June 3, 2003, INS NSEERS had led to the identification and apprehension of 11 suspected terrorists and denial of admission to more

than 765 aliens at our ports of entry who presented law enforcement threats due to outstanding felony warrants or prior criminal or immigration violations rendering them inadmissable.

The USA PATRIOT Act seeks to protect America from terrorist acts while preserving our civil liberties. We have vigilantly employed the sections of the PATRIOT Act which call for training of government officials and have found them most useful in ensuring that the employees of the United States government are not only able to do the job they are required to do, but also that they are supported in attaining those goals. Section 908 requires the Attorney General to establish a program to train government officials in the identification and use of foreign intelligence. Since December of 2002, the Department of Justice (OIPR, the Criminal Division, and the FBI) have worked alongside the CIA to create a FISA training program for Department lawyers and FBI agents involved with intelligence. The first of these four day National Security Conferences was held on May 6, 2003, and several others have been held since that time. Hundreds of prosecutors and agents have received this training to date. The Department of Justice is committed to the war on terrorism and appreciates the tools that Congress has provided through the USA PATRIOT Act.

b. Can you also tell us which have not proven particularly useful and why?

Answer: One provision of the USA PATRIOT Act that has not been particularly useful is Section 319(b), codified at 31 U.S.C. § 5318(k). This provision provides the authority to obtain foreign bank records from those foreign banks that maintain a correspondent bank in the United States.

While this authority has been authorized for use on one occasion to obtain foreign bank records, its usefulness is limited for a number of reasons. First, it is limited to administrative subpoenas. Unlike grand jury subpoenas, administrative subpoenas are not subject to the disclosure limitations of federal law. Therefore, the correspondent banks receiving administrative subpoenas may, and in some cases might be required, to disclose the receipt of the subpoena to the account holder. This is counterproductive to covert investigations because the use of an administrative subpoena will tip off the account holder, who is often the target of the investigation.

Second, the text of 31 U.S.C. § 5318(k) has been construed conservatively by the Justice Department to limit the use of these subpoenas to instances where there is a nexus between the funds deposited in a foreign bank and the correspondent account in the United States. Prosecutors are therefore faced with a high evidentiary threshold to obtain approval for these subpoenas as they often need the foreign records they seek in order to demonstrate the nexus with the correspondent account.

Finally, the use of a subpoena to obtain foreign bank records under this provision, like a Bank of Nova Scotia grand jury subpoena, is not approved where there is an alternative mechanism to

obtain the records, such as a mutual legal assistance treaty. In sum, this provision has the potential to be extremely useful in international financial crime and terrorism investigations.

c. Can you tell us which authorities have not been used?

Answer: The Department has not yet had an appropriate opportunity to use certain provisions of the USA PATRIOT Act, including (but not limited to) Section 806. Also, please refer to our answer to question 18, in which we note that, as of September 18, 2003, the FBI had not utilized Section 215 of the USA PATRIOT Act (relating to the production of business records).

While we have not yet had an appropriate opportunity to use Section 806, we expect that it will be highly useful in forfeiting the assets of terrorists, terrorist organizations and those who influence or support terrorism. By providing for the civil and criminal forfeiture of all assets, foreign and domestic, of any individual or organization engaged in terrorism and any assets used to commit or facilitate terrorist acts, Section 806 of the USA PATRIOT Act, codified at 18 U.S.C. § 981(a)(1)(G), is a tremendous tool for prosecutors. However, it has not been necessary for the Justice Department to seek forfeiture under this authority because the terrorist assets were frozen by OFAC. Forfeiture, unlike freezing, enables a court to transfer title to the United States. To date, none of the frozen assets have been forfeited to the United States, and it has not been appropriate to employ this powerful provision.

d. Are there any authorities changed in the USA PATRIOT Act that you recommend Congress reverse or further limit?

Answer: While there are no sections of the USA PATRIOT Act that the Department of Justice would recommend limiting or reversing at this time, we are reviewing certain sections for possible clarification. We look forward to continuing to work with the Congress on legislation which will assist our efforts in the war on terrorism

24. As Attorney General you are charged with protecting and defending the rights guaranteed to American citizens in the Constitution. That includes their safety and security, but it also includes their liberty and freedom.

a. What recommendations would you make to modify the changes made in the USA PATRIOT Act to better protect the liberty and freedom of U.S. persons without significantly compromising our need to protect safety and security?

b. Are their additional protections, beyond modification to the USA PATRIOT Act, that you can recommend to Congress to better protect our liberty and freedom?

Answer: Since the September 11th terrorist attacks, the Department of Justice has been unambiguous that its mission in the war on terrorism is a twofold one: preserving innocent lives while safeguarding the rights and liberties that are the birthright of every American. On September 17, 2001, less than a week after our nation came under attack, the Attorney General emphasized that "in our effort to make sure that law enforcement can gain the intelligence that it needs in order to protect America, we are also mindful of our responsibility to protect the rights and privacy of Americans." And in testimony before the House Judiciary Committee on September 24, 2001, the Attorney General stressed: "The fight against terrorism is now the highest priority of the Department of Justice. As we do in each and every law enforcement mission we undertake, we are conducting this effort with a total commitment to protect the rights and privacy of all Americans and the constitutional protections we hold dear."

For this reason, every anti-terrorism initiative launched in the past 29 months has been undertaken with a steadfast commitment to America's tradition of civil rights and liberties. For example, the revised Attorney General's investigative guidelines expressly instruct FBI agents to comply with all relevant laws, including the Constitution, when conducting investigations. And the guidelines flatly prohibit agents who visit public places and events from "maintaining files on individuals solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of any other rights secured by the Constitution or laws of the United States." Various provisions in the USA PATRIOT Act likewise provide that investigations of United States persons cannot be "conducted solely upon the basis of activities protected by the first amendment to the Constitution." In addition, the President's order establishing military commissions explicitly instructs that detainees must be "allowed the free exercise of religion," and specifically contemplates that any individuals tried before a commission will be represented by counsel.

25. The response from the Department of Justice to the Committee's questions concerning its use of the USA PATRIOT Act states that DOJ has used "sneak and peek" warrants on 47 separate occasions, and have sought to extend the period of delay for notice 248 times.

Have these warrants been used in ordinary criminal cases, such as drug prosecutions unrelated to terrorism? If so, how many times?

Answer: Section 213 of the USA PATRIOT Act allows courts to give delayed notice that a search warrant has been executed. This authority can be used only in certain narrow circumstances where immediate notification could result in serious harms, such as death, physical injury, flight from prosecution, or witness intimidation. In all cases, law enforcement is legally obligated to give notice that property has been searched or seized. In fact, it would be a violation of the USA PATRIOT Act to fail to provide notice after the court-approved period of delay has expired.

For years before the USA PATRIOT Act, courts had the legal authority to delay notice in a wide variety of ordinary criminal cases, including drug prosecutions. *See, e.g., United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990). But because of differences between jurisdictions, the pre-PATRIOT law was a mix of inconsistent standards that varied widely across the country. This lack of uniformity hindered complex terrorism cases. Section 213 thus did not *create* the authority for delayed notice on search warrants; that authority has been recognized by the courts in many cases for some time. Rather, section 213 resolved a problem by establishing a uniform statutory standard for the practice of delayed notice. And, of course, because the provision was codifying and making uniform an authority that had existed for use in any criminal case, section 213 did not impose a new restriction on that authority by needlessly limiting it to terrorism cases.

26. Some libraries have made a practice of destroying computer records and other records in defiance of the PATRIOT Act, saying that they don't agree with it. These institutions are attempting to make it more difficult for the Justice Department to come in and actually search those records.

a. Has any investigation been stymied as a result of this?

b. Has the Justice Department sought information that it learned has been destroyed by any of the libraries?

Answer: We are not aware of any information in our possession that would permit us to respond to either of these questions.

27. I have learned that university officials in Arizona have approached the FBI in an attempt to assist with ongoing investigations on students suspected of terrorism. The university administration asked if it might be able to provide needed information to the FBI. The FBI refused these offers.

What is the policy of the Justice Department in terms of cooperating with local officials outside of the law enforcement community who may have information that would be helpful to terrorism investigations?

Answer: The Phoenix Division of the FBI has an effective working relationship with the police departments of both major universities within its jurisdiction. The SAC and ASAC have met with executive level representatives from Arizona State University to discuss enhancing communications. ASU's police have identified an officer to become a full-time member of the Phoenix Joint Terrorism Task Force and a security clearance has been issued to the University's Chief of Police.

The Phoenix Division has identified only one event that may be the subject of this inquiry. In April 2003, the Phoenix Division Joint Terrorism Task Force executed an ATF search warrant on three ASU students. The warrant executions generated some press coverage and the field office was contacted by someone calling on behalf of the main Muslim student group at ASU. The group requested a meeting with FBI officials on the ASU campus, with the media in attendance. FBI officials declined this invitation, but did agree to meet with several members of the student group to discuss information regarding the case which would become publicly available. Before the meeting could take place, the warrants were sealed by the United States Attorney's Office thus negating any discussion of the case. FBI officials offered to meet with the students to discuss general terrorism topics. The field office was not recontacted and the situation was not discussed at the recent meeting between FBI and University officials.

28. In his report on 9/11 detainees, the IG explains that after September 11, the Justice Department was concerned about the possibility of additional sleeper cell attacks and that the FBI immediately sought to shut down any "sleeper" cells of terrorists who might be preparing another wave of violence.

a. Is this an accurate description of the Justice Department and FBI's focus following the September 11 attacks?

Answer: In the days, weeks and months after the terrorist attacks of September 11th, the FBI by necessity worked under the assumption, based on consistent intelligence reporting, that a second wave of attacks could be coming. We did not know where, when, or by whom, but we knew that the lives of countless Americans could depend on our ability to prevent that second wave of terror.

b. Isn't it the Department of Justice's duty to use all legal tools, including the Immigration and Nationality Act, to protect the American people from those who would come to our country with malevolent intentions?

Answer: The Department believes that it is best advised to use all legal tools at our disposal to detain, investigate and prosecute violations of our nation's laws and ensure that any threats to the American people are effectively handled. We believe this strategy should include legal tools such as the detention or removal powers authorized under the Immigration and Nationality Act. In addition, given the 87 percent absconding rate of non-detained illegal aliens, noted by the Inspector General in his February 2003 report, it would have been irresponsible to release aliens who were of interest to an ongoing terrorism investigation. With regard to the response in the event of a future terrorist attack, the Department of Justice is working with the Department of Homeland Security on a memorandum of understanding that would govern immigration cases of national security interest to the FBI and the Department of Justice.

29. The IG's report on 9/11 detainees quotes you as stating that even though some of the 9/11 detainees may have wanted to be released or may have been willing to leave the country, it was in the national interest to find out more about them before permitting them to leave.

a. What risk would it pose to the United States if our government were to allow a potential terrorist to leave our country without investigating the alien's possible ties to terrorism?

Answer: If, during the investigation into the attacks of September 11th, the government had released or granted bond to an illegal alien without fully investigating that individual's ties to terrorism, we might have risked another terrorist attack or the loss of an individual who possessed information relevant to the September 11th attacks. Instead, we proceeded with proper diligence and caution, conducting appropriate investigations before releasing or deporting these illegal aliens.

b. What risks would it pose to our relations with another country if we were to return a possible terrorist to that country without investigating the alien's terrorist ties and informing the home country of our government's findings?

Answer: The removal of aliens often raises foreign policy issues and these issues take on even greater significance when the U.S. government possesses information indicating that an individual alien has ties to terrorism. Information-sharing across governments is vital to the ongoing cooperative efforts of each country in light of the international coalition fighting the war on terrorism. In addition, each country needs to be aware of threats that could be posed by its own nationals. Therefore, a thorough investigation was determined to be appropriate for the September 11th detainees.

30. a. Do illegal aliens in the United States have an automatic right to release on bond during removal proceedings, or is release on bond a discretionary determination made in all cases by an appropriate officer after assessing whether the alien poses a risk to the national security?

Answer: Release on bond during removal proceedings is generally discretionary, Congress has mandated aliens previously convicted of certain offenses and those charged with removal under the security-related provisions must be detained until the removal proceedings are completed. Moreover, the standard for release is not whether an alien poses a risk to the national security: other considerations are to be taken into account. Finally, while DHS makes the initial decision whether to detain an alien during the pendency of removal proceedings, such aliens have a right to seek a redetermination of the DHS custody decision by an immigration judge, unless the alien is subject to mandatory detention. We will continue to work with DHS to provide information and other assistance for DHS's use in that process. As stated above, the Department of Justice is

working with the Department of Homeland Security on a memorandum of understanding that would govern immigration cases of national security interest to the FBI and the Department of Justice.

b. Wouldn't it have been irresponsible for the INS or Justice Department to release an alien who the FBI has reason to believe is connected to the September 11 attacks specifically or to terrorism generally?

Answer: Yes, the Department of Justice believes that it would have been reckless to release individuals encountered during the PENTBOM investigation without thoroughly investigating whether they had any connection to or information about the terrorist attacks of September 11th and whether that individual continued to pose a threat to the American people.

31. According to the Inspector General's report on September 11 detainees, there were 762 special interest detainees, of which 515 were deported after being "cleared" by the FBI. What does the word "cleared" mean? Is it true that an alien can be "cleared" for removal but still have connections to terrorism?

Answer: In some cases, the FBI and other law enforcement agencies were able to determine that aliens detained in connection with the September 11th investigation were no longer of investigatory interest, and those individuals were subsequently released or deported. In other cases, while there may have been information linking an individual to criminal or terrorist activity, the information was not substantial enough to prosecute and all indications were that no further substantive information would surface. In those cases, in the interest of national security, it was determined that the best course of action was to proceed with deportation, and remove a potentially dangerous person from our borders based upon an immigration violation rather than release the individual back into American society.

32. When Congress voted on the USA PATRIOT Act, it did so at the strong insistence of the DOJ that these new authorities were necessary in order to fight terrorism. It was further urged that the bill be enacted quickly so that we could get that fight underway. However, it is now clear that many of those new authorities are unnecessary in that regard. Now that we have had more time to look at the effectiveness of these authorities, we can see that some of them were improperly enacted. We can carefully review each new authority and determine which ones, if any, will actually be useful in fighting a war on terrorism. What steps are you planning to take to get this process going and to ensure that it is completed properly and in a timely manner?

Answer: The Justice Department's considered judgment is that the federal government's success in preventing another catastrophic attack on American soil in the 29 months since the September

11th atrocities would have been much more difficult – and perhaps impossible – without the USA PATRIOT Act. Our overall experience is that the new tools authorized by Congress in that Act have greatly strengthened our ability to prevent, investigate, and prosecute acts of terrorism.

Since the USA PATRIOT Act became law in October 2001, the Justice Department and the FBI have used many of its new authorities to investigate the September 11th terrorist attacks. Those tools also have proven equally valuable in our continuing efforts to detect and prevent terrorist acts before they occur, and to arrest and prosecute terrorists. Among other provisions, the Department and FBI have used the tools provided by the following sections of the Act: 201, 203, 205, 207, 209, 210, 211, 212, 216, 217, 218, 219, 220, 319, 373, 402, 403, 414, 416, 801, 805, and 905. Details about the use of these provisions were provided to the House Judiciary Committee in a letter from Acting Assistant Attorney General Jamie E. Brown dated May 13, 2003.

33. **The OIG report contains horrifying examples of mistreatment of detainees, including the taunting of detainees by calling them "Bin Laden junior" and telling them "you're going to die here," "someone thinks you have something to do with [9/11] so don't expect to be treated well." The detainees were physically abused as well- an inmate with a broken arm and injured finger had his wrist and finger twisted by officers, another was thrown in his cell naked without a blanket. They were deprived medical attention for injuries sustained in those assaults because, in the words of one physician's assistant, they "were not entitled to the same medical or dental care as convicted federal inmates." Your spokesperson said the Department makes "no apologies" for this conduct. Do you stand by her statement?**

Answer: As the Attorney General indicated before the House Judiciary Committee on June 5, 2003, the Department of Justice does not condone the abuse or mistreatment of any person being held in federal custody. The Department takes such allegations seriously and if any such allegations are found to be true, appropriate action will be taken. The statement of the Department's spokesperson applied to the overall detention policy: that we make no apologies that we detained illegal aliens when statistics show that 87 percent of them abscond when not detained. Again, it is not the policy of the Department to allow the mistreatment of anyone, particularly those persons in federal custody.

34. **Section 236A of the Immigration and Nationality Act makes an individual subject to mandatory detention as a person whom the Attorney General has reasonable grounds to believe is linked to terrorist activity, among other endangering activity. Custody under 236A requires "certification." Page 28 of the OIG report states that "as of March 26, 2003, no alien had been certified by the Attorney General under these provisions." Why were none of the 762 individuals certified under these provisions for custody?**

Answer: As you may be aware, section 236A of the Immigration and Nationality Act was added as a new provision to the immigration law by Section 412 of the USA PATRIOT Act. Although the Department contemplated using section 236A in a number of cases who presented national security risks following the President's signature of the USA PATRIOT Act into law on October 26, 2001, it was determined that it was unnecessary to use the new certification procedure because traditional administrative bond proceedings proved to be sufficient to detain individuals without bond.

35. What do you propose as a system for the Bureau of Prisons to report to the Department its policies and practices with respect to its treatment of immigration detainees?

Answer: We do not believe a new "system" is necessary for the Bureau of Prisons (BOP) to report to the Department on their policies and practices regarding the treatment of detainees: there is already good communication and coordination between the BOP and the Department on policy and practices in the area of Federal detention.

Federal detention affects several components within the Department, including the Bureau of Prisons, the United States Marshals Service, and the Detention Trustee's Office. There is a great deal of coordination between these components. The intra-departmental coordination included the Immigration and Naturalization Service until that component transferred to the Department of Homeland Security. We continue to coordinate detention issues with the Bureau of Immigration and Customs Enforcement in the Department of Homeland Security. Detention policies are one of many matters discussed and coordinated at meetings of representatives of these various agencies.

36. It is now some 20 months since the government arrested and detained over 1000 immigrants in the wake of 9/11. Nevertheless, the names of those detained are still being withheld. The main justification for this massive refusal to release information is that doing so will provide a "road map" to al Qaeda and other terrorist groups as to the investigations. However, in the program to interview Muslims, in the special registration program, in the absconders program, in the asylum program, it is clear that the focus was on Muslim men from certain countries. In light of that, why is it necessary to withhold the names of the detainees? It is said that there are national security reasons to withhold some of the names, but it should be possible to release the rest of the names.

Answer: On June 17, 2003, in Center for National Security Studies, et al. v. Department of Justice, the D.C. Circuit reaffirmed the Department's determination not to release the names of September 11th detainees, recognizing the serious nature of the harm that could flow from such

disclosure. Partial releases, above and beyond what the Department has determined to release, present potentially serious risks to national security and to the September 11 investigation. As the CNSS court noted, "[w]hile the name of any individual detainee may appear innocuous or trivial, it could be of great use to al Qaeda in plotting future terrorist attacks or intimidating witnesses in the present investigation." On January 12, 2004, the Supreme Court denied a writ of certiorari in this case. In addition, in some cases individual aliens might not wish to have it known that they were thought to be linked, at least initially, to a terrorism investigation.

U.S. Department of Justice

Washington, D.C. 20530

July 31, 2003

DEPARTMENT OF JUSTICE COMMENTS REGARDING THE DEPARTMENT OF THE TREASURY'S NOTICE OF INQUIRY RELATING TO CUSTOMER IDENTIFICATION PROGRAMS FOR FINANCIAL INSTITUTIONS SECTION 326 NOTICE OF INQUIRY: RECORDKEEPING RIN 1506-AA31

The Department of Justice (DOJ) hereby submits comments relating to the proposed new customer identification regulations with specific emphasis upon their potential impact upon terrorism, money laundering, identity theft, fraud, and their impact upon various law enforcement functions. The Department of Justice and the FBI have been charged by the President to protect the American people from the continuing threats of terrorism and the crimes associated therewith. We present our views and concerns in light of our experience and efforts following the attacks of September 11, 2001.

The Department of Treasury has asked for comments on two general issues: (1) whether and under what circumstances financial institutions should be required to retain photocopies of identification documents relied on to verify customer identity; and (2) whether there are situations when the regulations should preclude reliance on certain forms of foreign government-issued identification to verify customer identity. We address each area separately, as requested by the Notice of Inquiry.

Recordkeeping: Retention of Customer Identification Documents

The Department of Justice believes that there should be retention of photocopies of all documents utilized by regulated financial institutions for the purpose of verifying customer identities.

The attacks of September 11, 2001, have resulted in the need to be more vigilant in all environments, including business and financial transactions. Section 326 of the USA PATRIOT Act, Pub. L. No. 107-56 (Oct. 26, 2001), recognizes this reality and consequently requires, among other things, that financial institutions "maintain[] records of the information used to verify a person's identity, including name, address and other identifying information."

In response to the requirements directed by Congress, the Department of the Treasury issued a draft of proposed regulations in July of 2002. In the proposed rule, retention of photocopies of identity-verifying documents was specifically required. The final regulation, published on May 9, 2003, however, no longer required the retention of actual photocopies but rather allowed for a description of the type of document utilized to establish identity. The Department of Justice believes that this operational policy would undermine the effective investigation of terrorist-related activities, money laundering and identity theft, and potentially impair the prevention of criminal activities.

The crucial element in the acceptance of any identification document is the ability to verify the actual identity of the bearer of the card. In conjunction with law enforcement activities, we must be able to determine whether an individual is who he purports to be. This is essential in our mission to identify potential terrorists, locate their means of financial support and prevent acts of terrorism from occurring.

The primary law enforcement concern with the final rule's record retention requirement is that a mere description of an identity-verifying document provides little or no assistance in allowing law enforcement to investigate the actual identity of persons utilizing financial institutions. The current draft of the regulation allows for the potential use of bank accounts, without an adequate and easily accessible record of identification, by those intent upon engaging in criminal activity such as financing terrorist activities through the movement of funds, laundering money from drug trafficking or other criminal enterprises, and identity theft. Law enforcement has historically relied upon the ability to obtain copies of relevant identification documents, many of which contain photographs, to conduct an investigation to determine the true identity of an individual. Without a photograph or a photocopy of the identification document, it will be more difficult and, in some cases impossible, to pursue important investigative leads. Mere electronic descriptions of such documents would be of little use.

The Department of Justice strongly recommends that governing regulations be changed to revert back to the originally proposed rule (see 68 FR 25090) and to require the retention of photocopies of identity-verifying documents. Such copies should be retained under all circumstances which affect transactions that could be abused by potential terrorists and other criminal elements. The Department recognizes the concerns cited by FinCEN in the final regulation that resulted in the removal of the retention policy, but believes that these concerns are outweighed by the needs of law enforcement to be able to quickly and effectively identify criminals and terrorists who have used financial institutions to carry out their criminal, and in some cases deadly, activities.

If you wish to further discuss these comments, you may contact Julie Myers, Chief of Staff, Criminal Division, at (202) 353-3600 or Lester Joseph, Asset and Money Laundering Section, Criminal Division, at (202) 616-0593.